PAT-NO: JP410333839A
DOCUMENT-IDENTIFIER: JP 10333839 A
TITLE: FIBER CHANNEL CONNECTION STORAGE CONTROLLER

PUBN-DATE: December 18, 1998

INVENTOR-INFORMATION:

NAME	COUNTRY
SANADA, AKIYOSHI	
NAKANO, TOSHIO	
IWASAKI, HIDEHIKO	
SATO, MASAHIKO	
MURAOKA, KENJI	
TAKAGI, KENICHI	
KOBAYASHI, MASAAKI	

ASSIGNEE-INFORMATION:

NAME	COUNTRY
HITACHI LTD	N/A

APPL-NO: JP09140029
APPL-DATE: May 29, 1997

INT-CL (IPC): G06F003/06 , G06F003/06 , G06F012/14 , H04L012/56 , H04L012/22

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a fiber channel connection storage controller having a security function for preventing any illegal access from a host device in an environment in which access from all of host devices can be physically accepted.

SOLUTION: N Port Name information for uniquely identifying a host device is set in a microprocessor 42 of a storage controller 40 before the starting of host devices 10, 20, and 30. When the host

devices 10, 20, and 30 are started, and an issued frame is received by the storage controller 40, the microprocessor 42 operates comparison to detect whether or not the N Port Name information stored in this frame is registered in an N Port Name list in a control table already set and held in the microprocessor 42, and continues a processing based on the instruction of the frame when they are made coincident, and rejects the request when they are not made coincident. Thus, any illegal access from the host device can be suppressed, and the security can be held.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－333839

(43)公開日　平成10年(1998)12月18日

(51)Int.Cl.[6]		識別記号	FI		
G06F	3/06	304	G06F	3/06	304H
		540			540
	12/14	320		12/14	320F
H04L	12/56		H04L	11/20	102A
	12/22			11/26	

審査請求　未請求　請求項の数９　ＯＬ　（全 12 頁）

(21)出願番号　特願平9－140029

(22)出願日　平成９年(1997) ５月29日

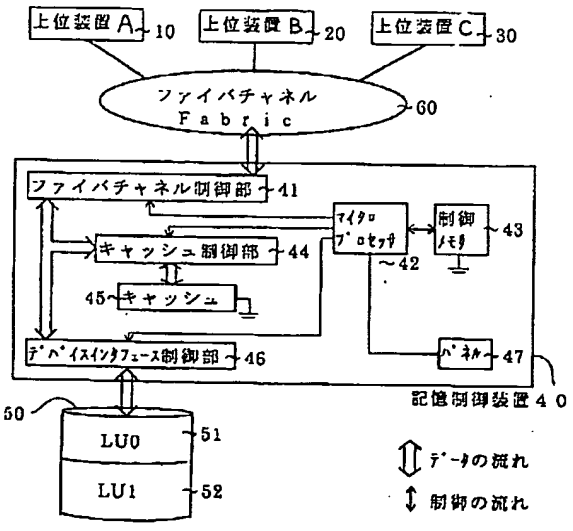
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　貫田　明美
神奈川県小田原市国府津2880番地株式会社日立製作所ストレージシステム事業部内
(72)発明者　中野　俊夫
神奈川県小田原市国府津2880番地株式会社日立製作所ストレージシステム事業部内
(72)発明者　岩崎　秀彦
神奈川県小田原市国府津2880番地株式会社日立製作所ストレージシステム事業部内
(74)代理人　弁理士　高橋　明夫　（外１名）

最終頁に続く

(54)【発明の名称】　ファイバチャネル接続記憶制御装置

(57)【要約】
【課題】　物理的にあらゆる上位装置からのアクセスを受け付けることが可能な環境の中で、上位装置からの不正なアクセスを防止するセキュリティ機能を持つファイバチャネル接続記憶制御装置を提供する。
【解決手段】　上位装置を一意に識別できるＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を、上位装置１０、２０、３０の立ち上がる以前に、記憶制御装置４０のマイクロプロセッサ４２に設定しておき、上位装置１０、２０、３０が立ち上がり、発行したフレームを記憶制御装置４０が受領した際、マイクロプロセッサ４２は、当該フレームに格納されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報が当該マイクロプロセッサ４２に既に設定され、保持されている制御テーブル内のＮ＿Ｐｏｒｔ＿Ｎａｍｅリストに登録されているかどうか、比較を行い、一致した場合は当該フレームの指示に基づく処理を継続し、不一致の場合は要求を拒絶する。これにより、上位装置からの不正アクセスを抑止することができ、セキュリティが保持できる。

図１



1

【特許請求の範囲】

【請求項1】ＡＮＳＩＸ３Ｔ１１で標準化されたファイバチャネルを、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び、記憶制御装置配下の磁気ディスクドライブで構成された記憶装置から成るコンピュータシステムにおいて、

上位装置から発行される、上位装置を一意に識別する情報であるＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を、上位装置の立ち上がる以前に記憶制御装置に設置しておき、記憶制御装置は当該情報を再設定されるまで恒久的に保持する手段を有し、上位装置が立ち上がった後、上位装置が、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報を格納したフレームを記憶制御装置に対して発行し、記憶制御装置がこれを受領した際、既に設定され、保持されている上位装置を一意に識別するＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報と、受領したフレームに格納されたＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報とを比較する手段を有し、比較により一致した場合、当該フレームの指示に基づく処理を継続し、不一致の場合、受領した当該フレームを拒絶するＬＳ＿ＲＪＴ（ＬｉｎｋＳｅｒｖｉｃｅ　Ｒｅｊｅｃｔ）フレームを上位装置に返し、上位装置からの不正アクセスを抑止する手段を有することを特徴とするファイバチャネル接続記憶制御装置。

【請求項2】請求項1記載のファイバチャネル接続記憶制御装置において、

当該記憶制御装置が有する上位インタフェース（ポート）の物理的な数以上のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を設定する手段、すなわち1ポートで複数のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を設定する手段を有し、ファイバチャネルＦａｂｒｉｃ接続時の論理パス多重構成にも上位装置からの不正アクセスを抑止する手段を有すことを特徴とするファイバチャネル接続記憶制御装置。

【請求項3】請求項2記載のファイバチャネル接続記憶制御装置において、

当該記憶制御装置の配下にディスクアレイ装置のように多くの磁気ディスクボリュームを有し、複数のチャネルパスルートを有するシステムにおいて、ＬＵＮ（ロジカルユニットナンバ）による論理ディスク領域、ＲＡＩＤグループによる論理ディスク領域、物理ボリューム領域等の記憶領域と、記憶制御装置のポートと、アクセス可能な上位装置のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報とを対応づけて管理する手段を有し、記憶領域毎に不正アクセスを抑止する手段を有することを特徴とするファイバチャネル接続記憶制御装置。

【請求項4】請求項2記載のファイバチャネル接続記憶制御装置において、

当該記憶制御装置配下の記憶装置が、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらのライブラリ装置のいずれかである場合に、当該記憶制御装置は、アクセス可能な上位装置、記憶制御装置のポート、記憶装置の対応付けを行い、ライブラリ装置の場合

2

はさらにドライブ、媒体の対応付けも行って、テーブルで管理、保持する手段を有し、上位装置からの不正アクセスを防止する手段を有することを特徴とするファイバチャネル接続記憶制御装置。

【請求項5】請求項1、2、3、4記載のファイバチャネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、パネルを用いて設定可能であることを特徴とするファイバチャネル接続記憶制御装置。

【請求項6】請求項1、2、3、4記載のファイバチャネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、パネルを用いて設定可能であり、さらに、当該情報の設定時の保護策を具備していることを特徴とするファイバチャネル接続記憶制御装置。

【請求項7】請求項1、2、3、4記載のファイバチャネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、上位装置のユティリティプログラムを用いて設定可能であることを特徴とするファイバチャネル接続記憶制御装置。

【請求項8】請求項1、2、3、4記載のファイバチャネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、上位装置のユティリティプログラムを用いて設定可能であり、さらに、当該情報の設定時の入力保護策を具備していることを特徴とするファイバチャネル接続記憶制御装置。

【請求項9】ネットワークアーキテクチャ形のチャネルを、複数の上位装置と、記憶制御装置との間のインタフェースとし、上位装置、記憶制御装置、及び、記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、

上位装置を一意に識別できる上位装置識別情報を、複数の上位装置の立ち上がる以前に、記憶制御装置に設定しておき、上位装置が立ち上がり、上位装置識別情報を格納しているフレームを発行し、当該フレームを記憶制御装置が受領した際、記憶制御装置は、当該フレームに格納されている上位装置識別情報が当該記憶制御装置に既に設定されているかどうか、比較を行い、一致した場合は当該フレームの指示に基づく処理を継続し、不一致の場合は要求を拒絶することを特徴とするチャネル接続記憶制御装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＡＮＳＩＸ３Ｔ１１で標準化されたファイバチャネルを上位装置とのインタフェースとする記憶制御装置に関し、特に上位装置、記憶制御装置及び当該記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、上位装置から当該

記憶制御装置に当該記憶装置へのアクセス要求があった際の、不正アクセス防止を行う記憶制御装置に関する。

【0002】

【従来の技術】ネットワーク上の不正アクセス防止に関しては、従来から種々の技術が知られている。

【0003】例えば、特開平3-152652号公報には、TCP/IPをサポートするコンピュータシステム間のネットワークセキュリティシステムとして、ログインできるユーザIDをメモリに定義しておくことにより、定義されたユーザID以外でログインしようとすると、そのネットワークを切断する機能を持たせることが開示されている。

【0004】また、特開昭63-253450号公報には、中央処理装置のオペレーティングシステムがユーザID、パスワード、回線アドレスをチェックすることにより、ディスク装置のファイルへの不正アクセス防止を行なうことが示されている。

【0005】さらに、IBM社のESCONインタフェースでは、上位装置が当該上位装置の論理アドレスをソースアドレスとしてフレームに格納し、送信してくることを利用して、記憶制御装置が事前に記憶制御装置に設定した論理アドレスとフレーム内の論理アドレスが一致するか否かをチェックする機能を設けている。

【0006】上述した従来技術は、上位論理層に1種類のレイヤを搭載するインタフェースを対象とした不正アクセス防止手段の域を出ないものである。

【0007】しかし、ANSIX3T11で標準化されたファイバチャネルは、ネットワーク形アーキテクチャであり、上位論理層にはTCP/IP、SCSI、ESCON、IPI等の種々のレイヤを搭載可能である。すなわち、データのフォーマットや内容には無関係に一台の装置から別の装置へバッファの内容を移すため、他のインタフェースと論理的に互換性を持ち、物理的に自由にアクセス可能である。特に、このファイバチャネルと、ディスクアレイ装置等の複数の記憶領域を有する記憶装置とを備えた記憶システムにおいては、上記記憶領域は多くの上位装置に共用される。したがって、従来の不正アクセス防止策では不十分であり、ユーザが意識したセキュリティ設定により、機密保持を行なう必要がある。

【0008】

【発明が解決しようとする課題】本発明は、ANSIX3T11で標準化されたファイバチャネルを、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び、この記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、物理的にあらゆる上位装置からのアクセスを受け付けることが可能な環境の中で、上位装置からの不正なアクセスを拒絶する手段を持たなかった記憶制御装置に対し、上位装置からの不正なアクセスを防止するセキュリティ機能を持つファイバチャネル接続記憶制御装置を提供することを目的とする。

【0009】さらに、本発明は、上位装置からの不正アクセス防止のために、アクセス可能な上位装置を容易に管理できる方式を持つファイバチャネル接続記憶制御装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明によれば、上記目的は、アクセス可能な上位装置の、上位装置を一意に識別するN_Port_Name情報を当該記憶制御装置に設定し、上位装置から送られてくるフレーム内に格納されたN_Port_Name情報と比較し、アクセスの可否を決定することにより達成される。

【0011】上記目的を達成するための本発明の具体的な特徴は、上位装置から発行される、上位装置を一意に識別する情報であるN_Port_Name情報を、パネル等を用いて入力し、入力情報を記憶制御装置の制御メモリに、制御テーブルとして格納する手段を有することである。この際、記憶制御装置は当該情報を再設定されるまで恒久的に保持する手段を有することが望ましい。

【0012】そして、上記制御テーブルを不揮発制御メモリに格納するようにすれば、万一の電源瞬断時にも管理情報を守ることができる。

【0013】さらに、本発明の具体的な特徴によれば、上位装置が立ち上がった後、上位装置がN_Port_Name情報を格納したフレームを記憶制御装置に対し発行し、記憶制御装置がこれを受領した際、記憶制御装置は既に設置され、保持されている上位装置を一意に識別するN_Port_Name情報と、受領したフレームに格納されたN_Port_Name情報とを比較する手段を有し、比較により一致した場合は、記憶制御装置は当該フレームの指示に基づく処理を継続し、不一致の場合は、受領した当該フレームを拒絶するLS_RJTフレームを上位装置に返すようにしたことである。これにより、記憶制御装置は上位装置からの不正アクセスを抑止することができる。

【0014】さらに、本発明の具体的な特徴によれば、当該記憶制御装置が有する上位インタフェース（ポート）の物理的な数以上のN_Port_Name情報を設定する手段を有することである。すなわち、1ポートで複数のN_Port_Name情報を設定する手段を有することである。これにより、ファイバチャネルファブリック（Fabric）またはスイッチ接続時の論理パス多重構成に対応できる。

【0015】また、当該記憶制御装置の配下に、ディスクアレイ装置のような、多くの磁気ディスクボリュームを有し、複数のチャネルパスルートを有すシステムにおいては、チャネルパスルート毎に、当該記憶制御装置配下のLUN（ロジカルユニットナンバ）による論理ディ

スク領域、物理ボリューム領域、ＲＡＩＤグループによる論理ディスク領域等の記憶領域と、記憶制御装置のポート、上位装置のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報との対応付けを記憶制御装置内で管理する手段を有することである。これにより、ユーザは、記憶領域毎に、不正アクセスを防止することができ、木目細かいアクセス管理が可能となる。

【００１６】さらに、本発明においては、記憶制御装置配下の記憶装置が磁気ディスク装置、ディスクアレイ装置の代わりに、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらの各種ライブラリ装置の何れの場合でも、当該記憶制御装置は、アクセス可能な上位装置のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報、記憶制御装置のポート、記憶装置の対応付けを行い、ライブラリ装置の場合はさらにドライブ、媒体の対応付けも行って、制御テーブルで管理、保持する手段を有し、フレーム受領の際にフレーム内の情報と制御テーブル内の情報を比較する手段を有し、上位装置からの不正アクセスの防止を行うことができる。

【００１７】さらに、本発明では、記憶制御装置が管理する情報を、パネル等を用いて設定する際、パスワードを入力する等により、管理情報を保護する手段を具備する。これにより、ユーザは当該情報の不正な登録、不正な再設定を防止することができる。また、ユーザは管理情報の設定を行うだけで、容易に不正アクセスを防止可能であり、ユーザの負担が少ない。

【００１８】なお、本発明において、記憶制御装置が管理する情報を設定する手段として、上述のように、パネル等を用いて設定する他に、上位装置のユティリティプログラムを用いて設定することも可能である。

【００１９】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。まず、図１ないし図５を用いて、本発明の対象となるファイバチャネル及びそれを用いて構成した記憶システムについて説明する。

【００２０】図１は、記憶制御装置配下の記憶装置がディスクアレイ装置の場合の記憶システムのハードウエア構成図である。図１において、１０、２０、３０は、データ処理を行う中央処理装置としての上位装置である。

【００２１】４０は、本発明を実施したディスクアレイ装置の記憶制御装置である。図１に示すように、記憶制御装置４０は、上位装置１０、２０、３０との間のデータ転送を制御するためのＤＭＡ（ダイレクト　アクセス　メモリ）を含むプロトコルプロセッサであるファイバチャネル制御部４１、記憶制御装置全体を制御するマイクロプロセッサ４２、制御装置の動作を制御するマイクロプログラム及び制御用データを保存する制御メモリ４３、キャッシュへのデータの読み書きを制御するキャッシュ制御部４４、書き込みデータ及びディスクドライブからの読み出しデータを一時バッファリングしておくディスクキャッシュ４５、ディスクドライブとの間のデータ転送を制御するためのＤＭＡを含むプロトコルプロセッサであるデバイスインタフェース制御部４６、装置構成情報を記憶制御装置へ入力するパネル４７から構成されている。

【００２２】５０は、記憶制御装置４０の配下にあるディスクアレイ装置である。ディスクアレイ装置５０は、上位装置のデータを格納する装置で、複数台の個別ディスクを冗長性を持つように配置構成したものである。

【００２３】ディスクアレイ装置５０を構成するディスクは、論理的に分割し、分割した区画をそれぞれ異なるＲＡＩＤレベルに設定することができる。この区画をＲＡＩＤグループという。このＲＡＩＤグループをさらに論理的に分割したＳＣＳＩのアクセス単位である領域をＬＵ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ）といい、その領域は、各々、ＬＵＮ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ）という番号を持つ。本実施の形態ではディスクアレイ装置５０は、ＬＵＮ０番のＬＵである、ＬＵ０（５１）とＬＵＮ１番のＬＵである、ＬＵ１（５２）の２個の領域を有する場合を示している。

【００２４】なお、ＬＵの数は、図１に示す２個に限らずもっと多くてもよく、シングルターゲット機能の場合、ターゲット当り最大８個までＬＵを設定できる。

【００２５】また、本実施の形態では、ＬＵなる記憶領域をアクセス単位としているが、アクセス単位とする記憶領域としては、物理ボリューム単位やＲＡＩＤグループ単位の記憶領域も可能である。

【００２６】上位装置１０、２０、３０と記憶制御装置４０は、ファイバチャネル６０をインタフェースとし、ファブリック（Ｆａｂｒｉｃ）という装置を介して接続されている。

【００２７】図１のシステムの動作を、上位装置１０が記憶制御装置４０経由でディスクアレイ装置５０とデータ転送を行う場合を例にとり、制御の流れ、データの流れを中心に説明する。

【００２８】上位装置１０がアクセス要求を出すと、その要求を認識したファイバチャネル制御部４１はマイクロプロセッサ４２に割り込み要求を発行する。マイクロプロセッサ４２は、上位装置からのコマンド情報及び本発明で必要な制御情報を、制御メモリ４３に格納する。

【００２９】コマンド情報が、ライトコマンドの場合は、マイクロプロセッサ４２はファイバチャネル制御部４１にデータ転送を指示し、転送されたデータをキャッシュ制御部４４を経由してキャッシュ４５に格納する。上位装置１０に対しては、ファイバチャネル制御部４１がライト完了報告を行う。ライト完了報告後、マイクロプロセッサ４２がデバイスインタフェース制御部４６を制御し、ディスクアレイ装置５０に対し、データ及び冗長データを書き込む。この場合、一般のＲＡＩＤ５の動作においては、旧データ、旧パリティ及び新データに基

いて新パリティを作成するが、本発明の制御によれば、マイクロプロセッサ４２が、デバイスインタフェース制御部４６及びキャッシュ制御部４４、制御メモリ４３、キャッシュ４５を用いて行なう。

【００３０】一方、上位装置１０からコマンド情報として、リードコマンド情報を受けた場合は、マイクロプロセッサ４２は、デバイスインタフェース制御部４６に指示を出し、当該アクセス要求のデータブロックが格納されたディスクアレイ装置５０へアクセスしてデータを読み出し、キャッシュ制御部４４を経由してキャッシュ４５へデータを格納する。マイクロプロセッサ４２は、ファイバチャネル制御部４１に指示を出し、ファイバチャネル制御部４１は、キャッシュ４５に格納したデータを上位装置１０に転送し、転送後上位装置へリード完了報告を行なう。

【００３１】次にファイバチャネル６０の特長を説明する。ファイバチャネルは最大１０ｋｍの距離で１００ＭＢ／ｓの転送が可能な高速インタフェースである。ファイバチャネルのアーキテクチャは転送元のバッファから転送先のバッファへデータを送るが、データのフォーマットや内容には無関係に一台の装置から別の装置へバッファの内容を移すため、異なるネットワーク通信プロトコルを処理するオーバヘッドがなく、高速データ転送を実現している。上位論理層にはＴＣＰ／ＩＰ、ＳＣＳＩ、ＥＳＣＯＮ、ＩＰＩ等の種々のレイヤを搭載可能である。すなわち、他のインタフェースと論理的に互換性を持つ。複雑な装置間の接続／交換という機能はＦａｂｒｉｃと呼ぶ装置が行ない、論理パス多重構成を組むことが可能である。

【００３２】ファイバチャネルがデータをやりとりする基本単位をフレームと言う。次に、このフレームについて、図２を用いて説明する。

【００３３】図２に示すように、フレーム７０は、スタートオブフレームＳＯＦ（Ｓｔａｒｔ　Ｏｆ　Ｆｒａｍｅ）７１、フレームヘッダ７２、データフィールド７３、サイクリックリダンダンシチェックＣＲＣ（Ｃｙｃｌｉｃ　ＲｅｄｕｎｄａｎｃｙＣｈｅｃｋ）７４及びエンドオブフレームＥＯＦ（Ｅｎｄ　Ｏｆ　Ｆｒａｍｅ）７５で構成される。

【００３４】ＳＯＦ７１は、フレームの先頭に置く４バイトの識別子である。

【００３５】ＥＯＦ７５は、フレームの最後につける４バイトの識別子で、ＳＯＦ７１とＥＯＦ７５によりフレームの境界を示す。ファイバチャネルではフレームがない時はアイドル（ｉｄｌｅ）という信号が流れている。

【００３６】フレームヘッダ７２は、フレームタイプ、上位プロトコルタイプ、送信元と送信先のＮ＿Ｐｏｒｔ＿ＩＤ情報、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報等を含む。Ｎ＿Ｐｏｒｔ＿ＩＤはアドレスを表わし、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅはポートの識別子を表わす情報である。

【００３７】データフィールド７３の先頭部には上位レイヤのヘッダを置くことができる。これにデータそのものを運ぶペイロード部が続く。ＣＲＣ７４は、フレームヘッダとデータフィールドのデータをチェックするための、４バイトのチェックコードである。

【００３８】上記フレームヘッダ７２のフォーマット８０を、図３に示す。フレームヘッダフォーマット８０において、デスティネーションアイデンティファイアＤ＿ＩＤ（Ｄｅｓｔｉｎａｔｉｏｎ　ＩＤ）８１はフレーム受け取り側のアドレス識別子であり、また、ソースアイデンティファイアＳ＿ＩＤ（Ｓｏｕｒｃｅ　ＩＤ）８２はフレーム送信側のＮ＿Ｐｏｒｔアドレス識別子であり、各々、Ｎ＿Ｐｏｒｔ＿ＩＤ、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報等を含む。

【００３９】次に図４を用いて、フレームを構成するデータフィールド７３のペイロードの１つである、ファイバチャネルプロトコルコマンドＦＣＰ＿ＣＭＮＤ（Ｆｉｂｒｅ　Ｃｈａｎｎｅｌ　Ｐｒｏｔｏｃｏｌ　ｆｏｒ　ＳＣＳＩ　Ｃｏｍｍａｎｄ）のペイロード９０の説明を行なう。

【００４０】ＦＣＰロジカルユニットナンバＦＣＰ＿ＬＵＮ（ＦＣＰ　Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ）フィールド９１には、コマンドを発行するロジカルユニット番号ＬＵＮが指定される。ＦＣＰコントロールＦＣＰ＿ＣＮＴＬ（ＦＣＰＣｏｎｔｒｏｌ）フィールド９２には、コマンド制御パラメータが指定される。そして、ＦＣＰ コマンドデスクリプタブロックＦＣＰ＿ＣＤＢ（ＦＣＰ　Ｃｏｍｍａｎｄ　Ｄｉｓｃｒｉｐｔｏｒ　Ｂｌｏｃｋ）フィールド９３には、ＳＣＳＩコマンドディスクリプタブロック（ＳＣＳＩ　Ｃｏｍｍａｎｄ　Ｄｅｓｃｒｉｐｔｏｒ　Ｂｌｏｃｋ）が格納され、リードコマンドＲｅａｄ等のコマンド種類、ＬＵＮ等のアドレス、ブロック数が示される。ＦＣＰデータレングスＦＣＰ＿ＤＬ（ＦＣＰ　Ｄａｔａ　Ｌｅｎｇｔｈ）フィールド９４には、当該コマンドにより転送されるデータ量がバイト数で指定される。

【００４１】以上のように構成されたフレームによってデータのやりとりが行われる。

【００４２】フレームは機能に基づいてデータフレームとリンク制御フレームとに大別される。データフレームは、情報を転送するために用い、データフィールドのペイロード部に上位プロトコルで使用するデータ、コマンドを搭載する。

【００４３】一方、リンク制御フレームは、一般に、フレーム配信の成功あるいは不成功を示すのに使われる。フレームを１個受領したことを示したり、ログインする場合に転送に関するパラメータを通知したりするフレーム等がある。

【００４４】次に、図５を用いて、「シーケンス」について説明する。ファイバチャネルにおけるシーケンス

は、あるN_Portから別のN_Portへ、一方向に転送される関連するデータフレームの集まりのことを言い、SCSIのフェーズに相当する。シーケンスの集まりをエクスチェンジと呼ぶ。例えばコマンドを発行して、そのコマンドの終了までに、そのコマンド実行のためにやりとりされるシーケンスの集まり（コマンド発行、データ転送、終了報告）がエクスチェンジとなる。このように、エクスチェンジはSCSIのI／Oに相当する。

【0045】図5（a）、（b）及び（c）は、それぞれ、ログインシーケンス（100）、リードコマンドシーケンス（110）及びライトコマンドシーケンス（120）を示す。

【0046】ファイバチャネルインタフェースでは、上位装置がデバイスに対し、通信パラメータを含むポートログインPLOGI（N_Port Login）フレームを送り、デバイスがこれを受け付けることで通信が可能となる。これをログインと呼ぶ。図5（a）に、ログインシーケンス（100）を示す。

【0047】図5（a）のログインシーケンス（100）において、まず、シーケンス101で、上位装置はデバイスに対し、PLOGIフレームを送り、ログインの要求を行なう。デバイスはアクノレッジACK（Acknowledge）フレームを上位装置に送り、PLOGIフレームを受け取ったことを知らせる。

【0048】次いで、シーケンス102において、デバイスは、ログイン要求を受け付ける場合はアクセプトACC（Accept）フレームを、要求を拒絶する場合はリンクサービスリジェクトLS－RJT（Link Service Reject）フレームを、それぞれ、上位装置に送る。

【0049】次に、図5（b）のリードコマンドのシーケンス（110）を説明する。

【0050】シーケンス111において、上位装置はデバイスに対し、FCP_CMNDフレームを送り、リード要求を行なう。デバイスはACKフレームを上位装置に送る。

【0051】シーケンス102では、デバイスは、FCPトランスファレディFCP_XFER_RDY（FCP Transfer Ready）フレームを上位装置に送り、データ転送の準備ができたことを知らせる。上位装置はACKフレームをデバイスに送る。

【0052】シーケンス113に進み、デバイスはFCPデータ（FCP_DATA）フレームを上位装置に送り、データを転送する。上位装置はACKフレームをデバイスに送る。

【0053】次のシーケンス114では、デバイスはFCP_RSPフレームを上位装置に送り、データの転送が正常終了したことを知らせる。上位装置はACKフレームをデバイスに送る。

【0054】次に、図5（c）のライトコマンドのシーケンス（120）を説明する。

【0055】シーケンス121において、上位装置はデバイスに対し、FCP_CMNDフレームを送り、ライト要求を行なう。デバイスはACKフレームを上位装置に送る。

【0056】次いで、シーケンス122において、デバイスはFCP_XFER_RDYフレームを上位装置に送り、データ書き込みが可能であることを知らせる。上位装置はACKフレームをデバイスに送る。

【0057】さらに、シーケンス123において、上位装置はFCP_DATAフレームをデバイスに送り、データを転送する。デバイスはACKフレームを上位装置に送る。

【0058】最後に、シーケンス123において、デバイスは、FCPレスポンスFCP_RSP（FCP Response）フレームを上位装置に送り、データの受け取りが正常終了したことを知らせる。上位装置はACKフレームをデバイスに送る。

【0059】以上、図1ないし図5によって、一般的なシステム構成、フォーマット及びシーケンスを説明したが、以下、本発明によるセキュリティチェックについて説明する。

【0060】初めに、PLOGI時におけるN_Port_Name情報を用いたセキュリティチェックについて、説明を行なう。

【0061】本発明では、図1において、まず、上位装置10、20、30の立ち上がる以前に、ユーザは記憶制御装置40のマイクロプロセッサ42にアクセス可能な上位装置のリストを設定する。すなわち、上位装置を識別できるN_Port_Name、N_Port_ID等の情報を、パネル47を用いて入力する。この際、パネルへの入力上の機密保護機能を実現するために、入力に際してパスワードを要求し、セキュリティを強化できる。

【0062】パスワードを入力し、既に設定したパスワードとの一致が図られた場合、記憶制御装置のポート毎にアクセス可能な上位装置のN_Port_Name情報を入力し、入力情報を制御テーブルに格納する。

【0063】いま、例として、上位装置10、20はディスクアレイ装置50にアクセス可能、上位装置30はディスクアレイ装置50にはアクセス不可能とし、N_Port_Nameを、上位装置10はHOSTA、上位装置20はHOSTB、上位装置30はHOSTCとし、記憶制御装置40のファイバチャネル制御部41のポートをCTL0P0とした場合、ログイン要求制御テーブル130は、図6のようになる。

【0064】図6に示すこのログイン要求制御テーブル130を、不揮発メモリ上に設定することにより、万一の電源瞬断時にも管理情報を守ることができる。

【0065】また、ログイン要求制御テーブル130に格納した情報は、電源を切断した場合はハードディスク領域50へ格納する。または情報の更新時にメモリ43とディスク50へ反映を行なう。これにより記憶制御装置40は、当該情報を再設定されるまで恒久的に保持することができる。

【0066】なお、ファイバチャネルにおいてノードやポートの識別に使用される自ノード情報として、N_Port_Nameの他に、N_Port_IDがあるが、N_Port_IDは変更される可能性があり、ユーザが管理する数値ではないため、N_Port_Name情報をセキュリティのためのチェック対象とするのが望ましい。

【0067】次に、図1及び図7を用いて上位装置のログイン要求に対する記憶制御装置のフレーム処理手順の説明を行なう。

【0068】（ステップS71）上位装置10、20、30が立ち上がり、各々、N_Port_Name情報を格納したログイン要求フレームであるPLOGIフレームを発行する。記憶制御装置40のマイクロプロセッサ42は、当該フレームを受領すると、まずこのフレームを受領したことを示すACKフレームを各上位装置に返す。

【0069】（ステップS72）そしてマイクロプロセッサ42は、当該フレームに格納されているN_Port_Name情報を切り出し、そのN_Port_Name情報が、既に設定され、保持されている制御テーブル内のN_Port_Nameリストに登録されているかどうか、比較を行なう。

【0070】（ステップS73）（ステップS74）（ステップS75）

上位装置10、20の発行した当該フレームに格納されているN_Port_Name情報は、制御テーブル内に登録されているN_Port_Name情報と一致するため、記憶制御装置40のマイクロプロセッサ42は、上位装置10、20に対してはログイン要求を受け付けた印として、ACCフレームを返し、ログイン処理を続行する。

【0071】（ステップS73）（ステップS76）

一方、上位装置30の発行した当該フレームに格納されているN_Port_Name情報は、制御テーブル内に登録されているN_Port_Name情報と一致しないため、記憶制御装置40のマイクロプロセッサ42は、上位装置30に対しては接続を拒絶するリジェクトパラメータをいれたLS_RJTフレームを返す。

【0072】以上のように、記憶制御装置40が、ログイン要求制御テーブル130を用いて、上位装置と記憶制御装置のポートの対応付けを管理することにより、ユーザはポート毎に上位装置からの不正アクセスを抑止することができ、セキュリティが保持できる。

【0073】次に、本発明において、ディスクアレイ装置の記憶領域であるLUN毎に、N_Port_Name情報を用いてセキュリティチェックを実施する方法について説明する。

【0074】本発明では、まず上位装置10、20、30の立ち上がる以前に、記憶制御装置40のマイクロプロセッサ42に、LUN毎にアクセス可能な上位装置のリストを設定する。上位装置を識別できるN_Port_Name、N_Port_ID等の情報を、パネル47を用いて入力する。この際、パネル47への入力上の機密保護機能を実現するために、入力に際してパスワードを要求し、セキュリティを強化することができる。

【0075】パスワードを入力し、既に設定したパスワードとの一致が図られた場合、LUN毎に記憶制御装置のポート及びアクセス可能な上位装置のN_Port_Name情報を入力し、入力情報を制御テーブルに格納する。

【0076】LU0（51）は、上位装置10から記憶制御装置40のファイバチャネル制御部41のポート経由でアクセス可能、LU1（52）は、上位装置20から記憶制御装置40のファイバチャネル制御部41のポート経由でアクセス可能とし、N_Port_Nameを、上位装置10はHOSTA、上位装置20はHOSTB、記憶制御装置40のファイバチャネル制御部41のポートをCTL0P0、とした場合、I／O要求制御テーブル140は、図8のようになる。

【0077】図8に示すこのI／O要求制御テーブル140は不揮発メモリ上に設定すると、万一の電源瞬断時にも管理情報を守ることができる。

【0078】また、図8のI／O要求制御テーブル140に格納した情報は、電源を切断した場合は、ハードディスク領域50へ格納する。または情報の更新時にメモリ43とディスク50へ反映を行なう。これにより記憶制御装置40は当該情報を再設定されるまで恒久的に保持することができる。

【0079】本実施例ではチャネルパスルートは1通りであるが、複数のチャネルパスルートを有するシステムにおいても同様である。

【0080】以下に図1及び図9を用いて、上位装置のI／O要求に対する記憶制御装置のフレーム処理手順の説明を行なう。上記の例ではPLOI時にセキュリティチェックを行なったが、本実施の形態では、各SCSIコマンド毎にチェックを行なう。

【0081】（ステップS91）上位装置10がLU0（51）にI／O要求を出したい場合、上位装置10は記憶制御装置40に対し、SCSI　CDBを格納したフレームを発行する。記憶制御装置40がこのフレームを受領した場合、まず、このフレームを受領したことを示すACKフレームを上位装置10に返す。

【0082】（ステップS92）そしてマイクロプロセ

ッサ42は、当該フレームに格納されているN_Port_Name情報及びCDB内のLUN番号を切り出し、そのN_Port_Name情報及びLUN番号が、当該マイクロプロセッサ42に既に設定され保持されている制御テーブル内のリストに登録されているかどうか、比較を行なう。

【0083】（ステップS93）（ステップS94）（ステップS95）

管理テーブル内には、「上位装置10は、LU0（51）をアクセス可能である」と登録されているため、記憶制御装置40のマイクロプロセッサ42はコマンドを受領し、I/O処理を継続する。

【0084】（ステップS91）一方、上位装置20が記憶制御装置40にLU0（51）のI/O要求フレームを発行し、記憶制御装置40がこのSCSI CDBを格納したフレームを受領した場合、マイクロプロセッサ42は、まずこのフレームを受領したことを示すACKフレームを上位装置20に返す。

【0085】（ステップS92）そしてマイクロプロセッサ42は、当該フレームに格納されているN_Port_Name情報及びCDB内のLUN番号を切り出し、そのN_Port_Name情報及びLUN番号が、管理テーブル内にあるかどうかの検索を行なう。

【0086】（ステップS93）（ステップS96）検索を行なった結果、管理テーブル内に、該当するLUNおよびN_Port_Nameの組合わせが存在しないため、記憶制御装置40のマイクロプロセッサ42は、上位装置20にLS_RJTフレームを送って、I/O要求を拒絶する。

【0087】こうして記憶制御装置は不正なアクセスを防止することができる。

【0088】ここではログイン及びI/O要求フレームを取り上げたが、これら以外の他の上位装置フレームに格納されているN_Port_Name情報を比較してもよい。

【0089】なお、ファイバチャネル接続記憶制御装置配下の記憶装置がディスクアレイ装置に限らず、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらのライブラリ装置である場合にも本発明を適用できる。

【0090】記憶制御装置配下の記憶装置が光ディスクライブラリ装置の場合に本発明を適用した場合の概要を図10を用いて説明する。150は記憶制御装置40配下の光ディスクライブラリ装置であり、151は光ディスクドライブ、152から156は光ディスクの媒体である。

【0091】ユーザは上位装置10、20、30が立ち上る前にパネルを使用して、媒体、ドライブ、ポートとN_Port_Name情報との対応付けを設定し、上位装置のアクセス権限をマイクロプログラムに保持しておく。

【0092】媒体152、153、154は、上位装置10からアクセス可能、媒体D155、E156は上位装置20からアクセス可能とし、N_Port_Nameを上位装置10はHOSTA、上位装置20はHOSTB、記憶制御装置40のポートをCTL0P0、光ディスクドライブA151をDRIVE0、媒体A152、B153、C154、D155、E156を各々MEDA、MEDB、MEDC、MEDD、MEDE、とした場合、要求制御テーブル160は、図11のようになる。

【0093】各上位装置がI/O要求フレームを発行した際、フレームを構成するペイロード内のCDBにボリューム情報が格納されているため、記憶制御装置40は当該フレームを受領した際、フレーム内のN_Port_Name情報及びペイロード内の媒体識別子を，当該記憶制御装置40に既に設定され、保持されている制御テーブルと比較を行なえばよい。このように、本発明を応用することによって、記憶制御装置は上位装置からの不正アクセスを防止可能である。

【0094】

【発明の効果】以上述べたように、本発明によって、ANSIX3T11で標準化されたファイバチャネルを上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、不正な上位装置からのアクセスを抑止することができるので、記憶装置内のデータの機密保護を行うことができる。

【0095】また、上位装置、記憶制御装置のポート、記憶領域を対応付けて上位装置からのアクセスを木目細かに管理できるので、記憶領域毎に用途を変える等、記憶装置をニーズに合わせて活用することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示すハードウエア構成図である。

【図2】第1の実施の形態におけるフレームのフォーマット図である。

【図3】図2で示したフレームを構成するフレームヘッダのフォーマット図である。

【図4】図2で示したフレームの一つであるFCP_CMNDのペイロードのフォーマット図（a）及び当該ペイロードを構成するFCP_CDBのフォーマット図（b）である。

【図5】第1の実施の形態において上位装置とデバイスがデータフレームのやりとりを行なうシーケンスの例を示し、ログイン時のシーケンス図（a）、リードコマンド時のシーケンス図（b）及びライトコマンド時のシーケンス図（c）である。

【図6】第1の実施の形態において、記憶制御装置が、上位装置を管理する制御テーブルを示した図である。

【図7】第1の実施の形態において、記憶制御装置が、上位装置（ホスト）からのログイン要求時に実行するフレーム処理のフローチャートである。

【図8】第1の実施の形態において、記憶制御装置が、記憶領域を管理する制御テーブルを示した図である。

【図9】第1の実施の形態において、記憶制御装置が、ホストからのI／O要求時に実行するフレーム処理のフローチャートである。

【図10】本発明の第2の実施の形態として、記憶制御装置配下の記憶装置が、光ディスクライブラリの場合を示すハードウエア構成図である。。

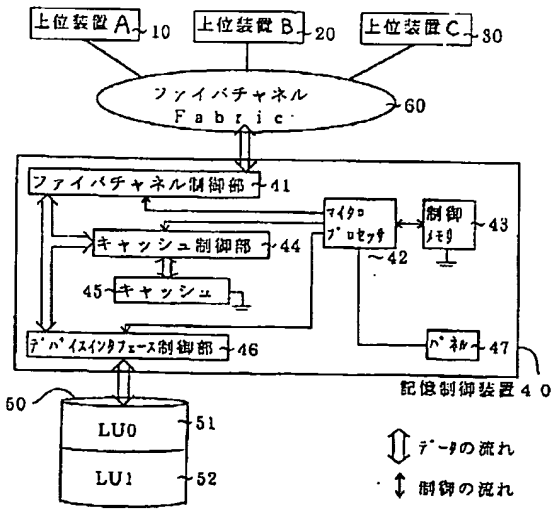
【図11】図10に示す第2の実施の形態において、記憶制御装置が管理する制御テーブルを示した図である。

【符号の説明】

10、20，30…上位装置、40…記憶制御装置、41…ファイバチャネル制御部、42…マイクロプロセッサ、43…制御メモリ、44…キャッシュ制御部、45…キャッシュ、46…デバイスインタフェース制御部、47…パネル、50…ディスクアレイ装置、51…ロジカルユニット0、52…ロジカルユニット1、60…ファイバチャネル、70…フレーム、71…スタートオブフレームSOF（Start Of Frame）、72…フレームヘッダ、73…データフィールド、74…サイクリックリダンダンシチェックCRC（Cyclic Redundancy Check）、75…エンドオブフレームEOF（End Of Frame）、80…フレームヘッダのフォーマット、81…デスティネーションアイデンティファイアD_ID（Destination ID）、82…ソースアイデンティファイアS_ID（Source ID）、90…ファイバチャネルプロトコルコマンドFCP_CMNDペイロード（Fibre Channel Protocol for SCSI Command）、91…ファイバチャネルプロトコルロジカルユニットナンバFCP_LUN（FCP Logical Unit Number）、92…ファイバチャネルプロトコルコントロールFCP_CNTL（FCP Control）、93…ファイバチャネルプロトコルコマンドデスクリプタブロックFCP_CDB（FCP Command Descriptor Block）、94…ファイバチャネルプロトコルデータレングスFCP_DL（FCP Data Length）、100…ログイン、110…リードコマンド、120…ライトコマンド、130…ログイン要求制御テーブル、140…磁気ディスクアレイI／O要求制御テーブル、150…光ディスクライブラリ、160…光ディスクライブラリI／O要求制御テーブル

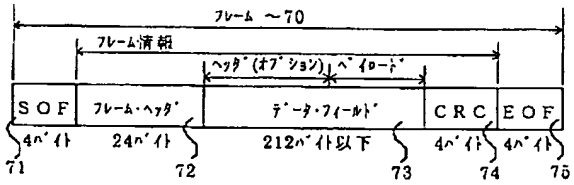
【図1】

図1



【図2】

図2



【図3】

図3

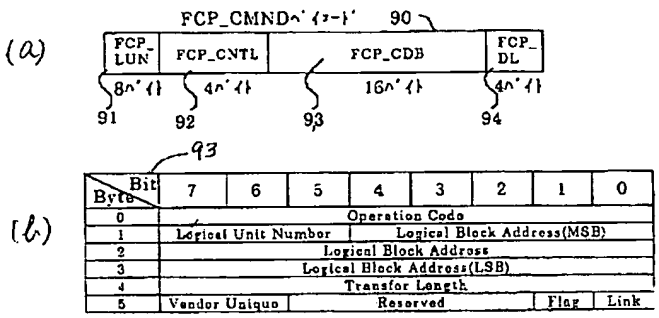
80

Bit / Byte	31-24	23-16	15-8	7-0
0	R_CTL	D_ID(フレーム受け取り側のN_Portアドレス識別子)		
1	Reserved	S_ID(フレーム送信側のN_Portアドレス識別子)		
2	TYPE	F_CTL		
3	SEQ_ID	DF_CTL	SEQ_CNT	
4	OX_ID		RX_ID	
5	Parameter			

81
82

【図4】

図4



【図6】

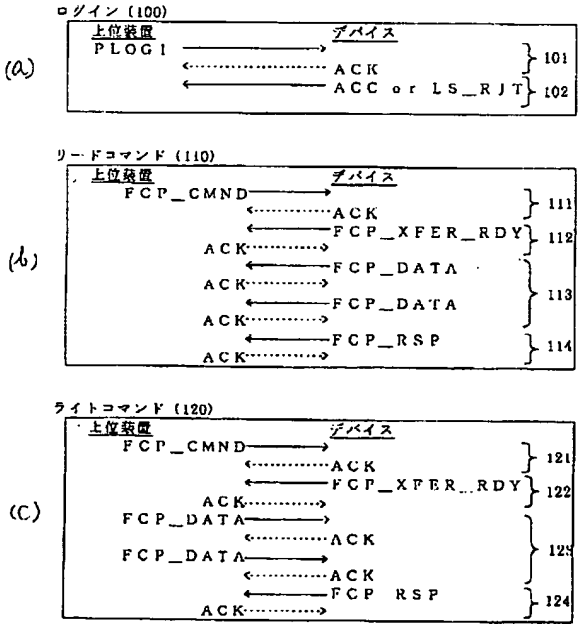
図6

制御テーブル 130

上位装置の N_Port_Name	記憶制御装置の 上位インタフェース(ポート)
HOSTA	CTL0P0
HOSTB	CTL0P0

【図5】

図5



【図8】

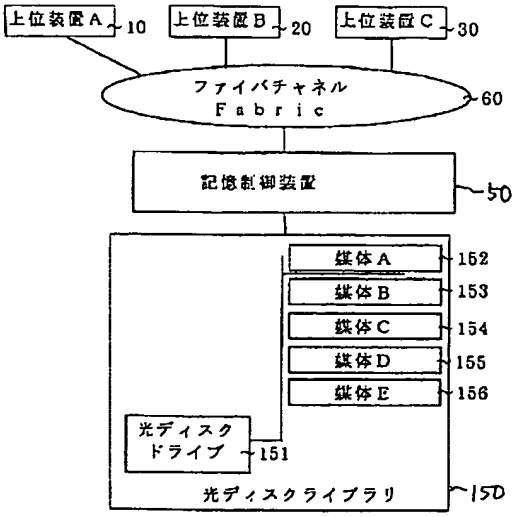
図8

制御テーブル 140

記憶領域 LU	上位装置の N_Port_Name	記憶制御装置の 上位インタフェース(ポート)
LU0	HOSTA	CTL0P0
LU1	HOSTB	CTL0P0

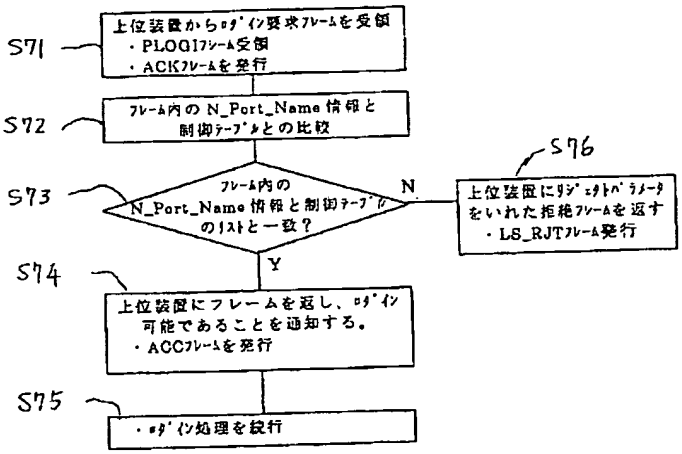
【図10】

図10



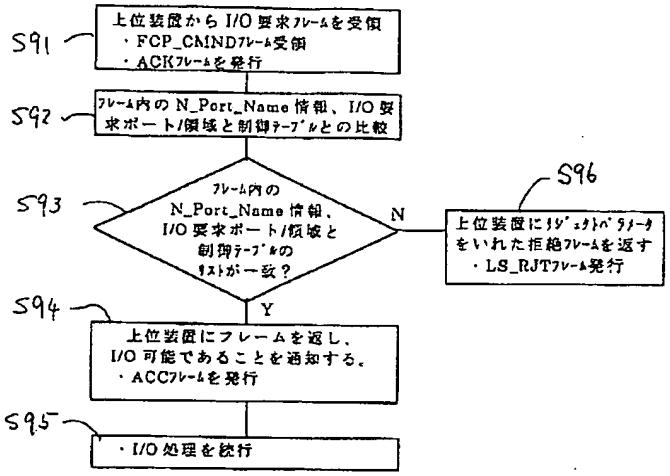
【図7】

図7



【図9】

図9



【図11】

図11

制御テーブル 160

記憶領域 光ディスク媒体	光ディスク ドライブ	上位装置の N_Port_Name	記憶制御装置の 上位インタフェース(ポート)
MEDA	DRIVE0	HOSTA	CTL0P0
MEDB	DRIVE0	HOSTA	CTL0P0
MEDC	DRIVE0	HOSTA	CTL0P0
MEDD	DRIVE0	HOSTB	CTL0P0
MEDE	DRIVE0	HOSTB	CTL0P0

フロントページの続き

(72)発明者 佐藤 雅彦
神奈川県小田原市国府津2880番地株式会社
日立製作所ストレージシステム事業部内
(72)発明者 村岡 健司
神奈川県小田原市国府津2880番地株式会社
日立製作所ストレージシステム事業部内
(72)発明者 高木 賢一
神奈川県小田原市国府津2880番地株式会社
日立製作所ストレージシステム事業部内
(72)発明者 小林 正明
神奈川県小田原市国府津2880番地株式会社
日立製作所ストレージシステム事業部内